NEBRASKA AUDITOR OF PUBLIC ACCOUNTS

Charlie Janssen
State Auditor

Charlie.Janssen@nebraska.gov
PO Box 98917
State Capitol, Suite 2303
Lincoln, Nebraska 68509
402-471-2111, FAX 402-471-3301
auditors.nebraska.gov

September 17, 2020

Jason Jackson, Director
Nebraska Department of Administrative Services
1526 K Street, Suite 240
Lincoln, Nebraska 68508

Dear Mr. Jackson:

This letter is provided pursuant to AICPA Auditing Standards AU-C Section 265B.A17, which permits the early communication of audit findings due to their significance and the urgent need for corrective action. The audit work addressed herein was performed as part of the fiscal year ended June 30, 2020, Comprehensive Annual Financial Report (CAFR) and Statewide Single (Single) audits. This communication is based on our audit procedures through June 30, 2020. Because we have not completed our audits of the fiscal year 2020 CAFR or Single, additional matters may be identified and communicated in our final reports.

In planning and performing our audits of the State's financial statements as of and for the year ended June 30, 2020, in accordance with auditing standards generally accepted in the United States of America, we considered the State's internal control over financial reporting (internal control) as a basis for designing the audit procedures that are appropriate in the circumstances for the purpose of expressing our opinions on the financial statements, but not for the purpose of expressing an opinion on the effectiveness of the State's internal control. Accordingly, we do not express an opinion on the effectiveness of the State's internal control.

Our consideration of internal control was for the limited purpose described in the preceding paragraph and was not designed to identify all deficiencies in internal control that might be material weaknesses or significant deficiencies and, therefore, material weaknesses or significant deficiencies may exist that were not identified. However, as discussed subsequently, based on the audit procedures performed through June 30, 2020, we identified certain deficiencies in internal control that we consider to be significant deficiencies.

We noted certain internal control or compliance matters related to the activities of the Nebraska Department of Administrative Services (Department), or other operational matters, which are presented below for your consideration. The following comments and recommendations, which have been discussed with the appropriate members of the agencies and their management, are intended to improve internal control or result in other operating efficiencies.

A deficiency in internal control exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct misstatements on a timely basis. A material weakness is a deficiency, or a combination of deficiencies in internal control, such that there is a reasonable possibility that a material misstatement of the entity's financial statements will not be prevented, or detected and corrected, on a timely basis.

A significant deficiency is a deficiency, or a combination of deficiencies, in internal control that is less severe than a material weakness, yet important enough to merit attention by those charged with governance. We consider Comment Numbers 1 (Human Resources User Role 65 & E1 Pay Rate Override), 2 (E1 Special Handle a Voucher), 3 (Changes to Vendor and Banking Information), and 4 (E1 Timesheets) to be significant deficiencies.

Draft copies of this letter were furnished to the Department to provide management with an opportunity to review and to respond to the comments and recommendations contained herein. All formal responses received have been incorporated into this letter. Responses were not subjected to the auditing procedures applied in the audit of the financial statements and, accordingly, the auditor does not express an opinion on them. Responses have been objectively evaluated and recognized, as appropriate, in the letter. Responses that indicate corrective action has been taken were not verified at this time, but they will be verified in the next audit.

The following are our comments and recommendations for the year ended June 30, 2020.

1. Human Resources User Role 65 & E1 Pay Rate Override

During the audit, we noted 329 payroll batches that were prepared, approved, and posted by a single DAS employee.

The Human Resource User Role 65 (HR 65) in EnterpriseOne (E1), the State's accounting system, was used by the Department to perform the final update processing for payroll. Six of the eight DAS employees with HR 65 access, were also able to prepare, approve, and post their own batches in E1. As a result of this access, we noted 329 payroll journal entries and vendor payroll deduction batches, including batches that contained DAS payroll, that were prepared, approved, and posted by a single DAS employee.

Additionally, we noted 997 users with access to add, change, and delete information in the Speed Time Entry screen in E1, which provided the ability to override pay rates, including their own, without approval. The Department did implement a process to review agency pay rate overrides starting in February 2020.

The Auditor of Public Accounts (APA) reviewed the override query for one pay period and noted over 27,600 overrides for 10 State agencies, with 27,535 overrides related to two of these agencies. The Department reviewed only three overrides related to one agency, which was inadequate to ensure that the overrides were appropriate.

Good internal control requires procedures to ensure an adequate segregation of duties, so at least two individuals are involved in processing payroll payments, and no one has the ability to adjust his or her own pay rate.

A lack of such procedures increases the risk of loss or misuse of State funds due to fraudulent activity within E1.

A similar finding was noted in the previous audit.

> We recommend the Department implement procedures to ensure any batches involving payroll are processed by at least two individuals. We also recommend the Department review options for disabling the ability of users to override pay rates, or implement adequate compensating controls to identify and review instances of overrides to pay rates.

Department Response:

Human Resource User Role 65: State Accounting has established compensating controls incorporating procedures to review the activity of those DAS employees assigned User Role 65, who have responsibility for processing internal payroll batches. DAS continues to work to minimize the number of times payroll batches are processed by one person.

E1 Pay Rate Override: State Accounting has established procedures to periodically review the use of pay rate overrides. Any entry that looks questionable is brought to the State Accounting Administrator's attention so further action can be considered. Of the 27,535 records noted, 932 were actual overrides. All appeared to be needed to record on call hours paid at rates between $1.11 and $2.63 per hour. State Accounting will review the Kronos interface process to determine if false positives can be eliminated.

2. E1 Special Handle a Voucher

The Special Handle a Voucher Function (Function) in E1 allows users to change the payee of a payment voucher without going through the batch management process. The Function is used by the following:

- The Department to provide support to agencies, so payments can continue in a timely manner if the agency lacks adequate personnel to process a transaction;

- The Department to process replacement warrants; and

- State agencies to correct vouchers without having to void and recreate another voucher.

We noted several issues with the Function in E1, including the following:

- Access to the Function is not restricted to only high-level users. Access was available, instead, to users who had access to Accounts Payable (AP) roles 20, 21, 30, 40, 41, 50, and 51. Essentially, anyone who had access to AP in E1, with the exception of inquiry-only access, was able to use the Function. Due to the type of activity that can be performed with this access, we believe access should be restricted to only a limited number of high-level users. Our review noted that 808 users had access to the Function as of March 11, 2020.

- Users with the ability to add vendors and change vendor information in E1 also had access to the Function. The Address Book (AB) 50 role allowed users to add venders and make changes to vendor information. All six users with AB 50 access also had access to the Function, creating an environment in which a user could set up fictitious vendors in the system or improperly change vender information and then change payee information on vouchers to direct payment to the fictitious/modified vendor.

The Department stated it uses the payee control-approval process in E1, a required step in payment processing, to review and approve vendor changes made through the Function; however, we noted the following issues related to the payee control-approval process:

- All eight users with access to the payee control-approval process also had access to the Function. Thus, these users could change a payee on a voucher and then approve it, without involvement of a second person, resulting in a lack of segregation of duties.

- One user with access to the payee control-approval process also had access to the Function and could add vendors or change vendor information in E1.

Nebraska Information Technology Commission (NITC) Standards and Guidelines, Information Security Policy 8-303 (July 2017), "Identification and authorization," states, in relevant part, the following:

> *(4) To reduce the risk of accidental or deliberate system misuse, separation of duties must be implemented where practical. Whenever separation of duties is impractical, other compensatory controls such as monitoring of activities, increased auditing and management supervision must be implemented. At a minimum, the audit of security must remain independent and segregated from the security function.*

Additionally, good internal control requires procedures to ensure an adequate segregation of duties, so no one individual is able to perpetrate and/or to conceal errors, irregularities, or fraud.

Without such procedures, there is an increased risk for errors or fraud to occur and remain undetected.

A similar finding was noted in the previous audit.

We recommend the Department implement procedures to ensure an adequate segregation of duties. Such procedures include: 1) restricting Function access to only certain high-level users; 2) removing access to the Function for users with the ability to add vendors and make changes to vendor information in E1; 3) maintaining documentation to support review/approval of vendor changes through the payee control approval process; and 4) preventing users with access to the payee control approval process from accessing the Function and/or adding/changing vendor information in E1.

Department Response: State Accounting will continue to review compensating control processes and procedures related to Payee Control and Special Handle a Voucher functions. As noted in the finding, only one user has access to the payee control-approval process, Special Handle a Voucher, and vendor address book records. If the vendor/payee is changed on a voucher, another user does complete a review and documentation from the agency is retained.

3. Changes to Vendor and Banking Information

In the prior year audit, the APA was informed of three erroneous payments resulting from unauthorized changes to an employee's and vendor's banking information that resulted from a lack of controls over such changes.

During our review of the process to change vendor and banking information in E1, we noted a lack of controls to ensure that additions and/or changes to vendor addresses and banking information were proper and accurate. To change vendor addresses and banking information in the system, an authorized agent at the agency level submits a W-9/ACH form to the Department. This submission can be made by a single person at the agency. There is no required secondary approval of changes at the agency level to ensure additions and changes are proper.

In addition, we noted that the Department did not perform any other procedures to identify potential fraudulent bank accounts in the system. A review could include querying for duplicate bank accounts or addresses existing for both a vendor and employee of the State.

A good internal control plan requires procedures to ensure that critical vendor and banking information within E1 is proper, and changes to that information are verified as accurate.

Without such procedures, there is an increased risk of loss, misuse, or theft of State funds due to fraudulent activity within E1.

A similar finding was noted in the previous audit.

We recommend the Department establish procedures to ensure vendor addresses and banking information in E1 are appropriate and accurate. These procedures should require a secondary approval of all vendor and banking information at the agency level when modifying W-9/ACH forms, ensuring that at least two knowledgeable individuals are involved in the changes. We also recommend the Department establish procedures, such as a periodic review for duplicate bank accounts and vendor addresses, to identify potential fraudulent bank accounts in the system.

Department Response: DAS continues to review and improve procedures for vendor set-up and maintenance, including accuracy of vendor records. As a control that DAS already has in place, changes to a vendor/payee's banking information requires prior banking information be provided for verification.

4. E1 Timesheets

Twenty State agencies utilized E1 to record their employees' work time entry and leave reporting. For these agencies, we noted the following:

- Overtime-exempt employees were not required to maintain a timesheet or other form of documentation to show that at least 40 hours were worked each week. Exempt employees were required to record only leave used in the system.

- E1 timesheets were maintained only for the current pay period for 17 State agencies and one year for one State agency that used the time entry function in E1.

- Supervisors and human resource staff within the State agencies were able to change the employees' submitted timesheets without the employees' knowledge or documentation of the changes made.

- E1 did not accurately track who approved timesheets in the system. Each employee was assigned a supervisor in his or her master file in the system. For State agencies that utilized timesheet entry in E1, the supervisor assigned to an employee approved the timesheet. However, supervisors were allowed to set up delegates in the system to approve timesheets in the supervisor's absence. The system did not record who actually approved the timesheet; if a delegate approved an employee timesheet, the system would record the assigned supervisor as the approver. When delegates were set up for their supervisor, the delegate was then able to alter and approve his or her own timesheet. Furthermore, there was no audit trail for delegates in E1. When a supervisor terminated, there was no record of the delegates in the system. Supervisors were also able to delete delegates without any record of the assignment.

- Employees were able to record their time worked to other agency funding sources. When completing a timesheet, the employee had a field available to him or her to record time to any State agency. The coding was not restricted to only the employing agency.

A similar finding was noted in the previous audit.

Neb. Rev. Stat. § 84-1001(1) (Reissue 2014) states the following:

> *All state officers and heads of departments and their deputies, assistants, and employees, except permanent part-time employees, temporary employees, and members of any board or commission not required to render full-time service, shall render not less than forty hours of labor each week except any week in which a paid holiday may occur.*

Sound business practices, as well as a good internal control plan, require hours actually worked by State employees to be adequately documented and such documentation to be kept on file to provide evidence of compliance with § 84-1001(1). Furthermore, a good internal control plan requires employers of employees who accrue vacation and sick leave to maintain adequate support that employees actually earned the amounts recorded in their leave records.

Section 124-86, Payroll – Agency Records, of Nebraska Records Retention and Disposition Schedule 124, General Records (February 2020), as issued by the Nebraska State Records Administrator, requires any "supporting records received or generated by an agency used to review, correct or adjust and certify agency payroll records" to be retained for five years. Per that same section, the supporting records may include timesheets and reports.

Good internal control requires procedures to ensure that the approval of timesheets is documented for subsequent review, and business units are restricted to an employee's agency.

Without such procedures, there is an increased risk for fraudulent or inaccurate payment of regular hours worked or accumulation of leave. Additionally, failure to retain important payroll documentation risks noncompliance with Nebraska Records Retention and Disposition Schedule 124. When business units are not restricted, there is an increased risk that an employee may record payroll expenditures to an incorrect funding source or another agency's general ledger in error.

We recommend the Department establish a policy requiring State agencies to maintain adequate supporting documentation of time worked for all employees, such as timesheets or certifications, in compliance with Nebraska Records Retention and Disposition Schedule 124. Furthermore, we recommend the Department make the necessary changes to E1, or save supporting documentation to a data warehouse, to allow for the retention of timesheets, documentation of approvals, and changes to timesheets to ensure compliance with Nebraska Records Retention and Disposition Schedule 124. Lastly, we recommend the Department restrict business units to an employee's agency.

Department Response: Timesheet images are maintained in EnterpriseOne until the payroll is processed; however, the electronic data is maintained in EnterpriseOne indefinitely. Agencies will be reminded to retain any information they may receive, generate or create outside of EnterpriseOne in support of an agency's payroll to be done in accordance with the Nebraska Records Retention and Disposition Schedule 124.

5. E1 Business Continuity Plan

The Department has not recently tested its process to ensure timely, continued operations of the State's accounting system, E1, at its backup site in the event the application fails at its main location. The Department last tested this process in March 2018.

A good internal control plan and sound business practices require procedures to ensure business continuity plans are tested periodically. Furthermore, the Information Systems Audit and Control Association (ISACA) has published the Control Objective for Information and Related Technology (COBIT) 2019 framework, which is a nationally recognized information system framework.

COBIT 2019, DSS04.04 Exercise, test and review the business continuity plan (BCP) and disaster response plan (DRP), states, in part, the following:

Test continuity on a regular basis to exercise plans against predetermined outcomes, uphold business resilience and allow innovative solutions to be developed . . . .

1. *Define objectives for exercising and testing the business, technical, logistical, administrative, procedural and operational systems of the plan to verify completeness of the BCP and DRP in meeting business risk.*

2. *Define and agree on stakeholder exercises that are realistic and validate continuity procedures. Include roles and responsibilities and data retention arrangements that cause minimum disruption to business processes.*

3. *Assign roles and responsibilities for performing continuity plan exercises and tests.*

4. *Schedule exercises and test activities as defined in the continuity plans.*

5. *Conduct a post-exercise debriefing and analysis to consider the achievement.*

6. *Based on the results of the review, develop recommendations for improving the current continuity plans.*

When periodic testing is not performed, there is an increased risk of prolonged interruption of government operations, in the event of a disruption or failure.

We recommend the Department implement effective business continuity controls, including periodic testing of existing recovery procedures to ensure continuity of operations of the State's accounting system in the event of disruption or failure.

Department Response: DAS Business Continuity and System Security Plans have been updated. An internal continuity exercise is planned for September 23, 2020.

6. Workday User Access

Workday is the State's Human Resources (HR) system. Users assigned to Workday roles or security groups are given elevated access within Workday. In order to receive access to a Workday role or security group, a security partner at a State agency submits an email request that is approved by either the Department HR Systems Coordinator or the Department Personnel Program Administrator. However, during our testing of users' assigned Workday roles and security groups, we noted the following:

- For three of nine users, no documentation was on file to support that the State agency security partner requested the access granted. For these same three users, documentation was not on file to support that the Department HR systems Coordinator or the Personnel Program Administrator approved the access granted.

- The Department lacked a formal process for requesting and approving access to Workday security groups.

Furthermore, we noted that the Department did not perform a periodic review of elevated users' access in Workday in order to ensure those with the elevated access needed it as part of their job duties.

A good internal control plan requires a formal request and approval process for giving users elevated access in applications. Furthermore, good internal controls require the performance of periodic reviews to ensure that only proper individuals are provided elevated access.

Nebraska Information Technology Commission (NITC) Technical Standards and Guidelines, Information Security Policy 8-502(1) (July 2017), "Minimum user account configuration," states the following, in relevant part:

> *User accounts must be provisioned with the minimum necessary access required to perform duties. Accounts must not be shared, and users must guard their credentials.*

Good internal control requires a formal process for requesting, approving, and reviewing user access to applications.

Without such procedures, there is an increased risk of users being granted unauthorized access.

A similar finding was noted in the previous audit.

> We recommend the Department implement procedures for requesting and approving Workday roles and security group access. Those same procedures should also provide for reviewing periodically, at least annually, user access to Workday.

Department Response: Formal procedures for requesting and approving group access are in place. When an agency needs a teammate to have new/updated access in Workday, they send a request to NIS.Security. NIS.Security forwards that request to State Personnel for review and approval or denial. A process is in place for verifying a position still needs role access when a user terminates. When someone terminates employment, the "NIS.Security team" removes the Role Assignments on that vacated position, unless the termination event is rescinded based on a request from the agency.

APA Response: The process explained by DAS was not documented in formal policies or procedures, and DAS was unable to provide documentation showing the access granted to the users tested was requested and approved.

7. E1 Terminated User Access

The APA ran a query to identify terminated users of E1 whose access was not removed in a timely manner. The query parameters identified 53 terminated employees whose access was removed more than five business days after they terminated employment.

The APA selected 10 employees from the list of 53 to verify that their access was not removed timely. For the 10 selected, the agency failed to notify the Department within five business days of the employees' termination dates. The number of business days it took to remove the 10 users' access ranged from 6 to 125 days. Additionally, 1 of the 10 employees appears to have logged into E1 after the employee's termination date.

The Department is responsible for disabling a user's access to E1 when that employee terminates; however, for these terminated users, the Department was not notified in a timely manner to remove the access. The Department is notified when the State agency for which the employee worked enters a termination date into Workday (the State of Nebraska's Human Resources system). Without timely notification, the Department is unable to remove the access expeditiously. For the users noted, the Department removed their E1 access within three business days of receiving notification of termination.

Nebraska Information Technology Commission (NITC) Technical Standards and Guideline, Information Security Policy 8-701 (July 2017), "Auditing and compliance; responsibilities; review," states the following, in relevant part:

> *An agency review to ensure compliance with this policy and applicable NIST SP 800-53 security guidelines must be conducted at least annually.*

National Institute of Standards and Technology (NIST) Special Publication 800-53, Security and Privacy Controls for Federal Information Systems and Organizations, Access Control 6 (AC-6), Least Privilege, states, in part the following:

> *The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.*

Nebraska State Accounting Manual, AM-005, General Policies, Section 32, Terminated Employee Payroll and Financial Center ID's, states the following, in relevant part:

> *Each agency shall have a documented procedure to immediately disable the Payroll and Financial Center [EnterpriseOne] ID of an employee who has terminated employment with the agency. It is the responsibility of the agency's authorized agent to request termination of the User ID from the computer system within five working days from the termination date . . . .*

Good internal control requires procedures to ensure the timely removal of terminated users' access to E1.

Without such procedures, there is an increased risk of inappropriate access to State resources, as well as unauthorized processing of transactions.

A similar finding was noted in the previous audit.

> We recommend the Department work with State agencies, through on-going training and monitoring of agency personnel, to ensure agencies request termination of E1 users IDs prior to, or immediately upon, termination. We recommend agencies trigger such requests by entering employee termination dates in Workday as soon as a termination date is determined.

Department Response: DAS will continue to provide multiple training events during which agency personnel are reminded to enter termination dates in a timely manner, to facilitate the deactivation and termination of a user's EnterpriseOne access.

8. Clarity to E1 Timesheets

The Office of the Chief Information Officer (OCIO) used the Clarity program to record time worked and leave taken. Employees entered hours worked and leave used, which was then approved by their supervisor or delegate.

After the timesheets were approved, the hours were uploaded to E1 for payment. From E1, the Department HR created a payroll register and reviewed it for accuracy. However, the Department lacked a process for ensuring that the hours uploaded from Clarity were recorded correctly in E1.

The APA performed a reconciliation of two biweekly pay periods and identified the following issues:

- One employee entered her time in Clarity, but the time was not uploaded into E1. Her timesheets in E1 defaulted to 80 hours of regular pay each pay period regardless of the leave recorded in Clarity. After the APA brought this to the Department's attention, an adjustment was made to reduce the employee's sick leave balance by 112 hours and vacation leave balance by 86 hours; however, the adjustment did not include 12 hours of sick leave that the employee had used.

- One employee had an improper adjustment that reduced her paycheck by three regular hours. On the pay period tested, the Department HR made an adjustment to change some of the employee's sick leave to FMLA sick leave and reduced regular hours by three. As a result, the employee had three additional hours recorded as sick leave that was not supported.

Good internal control requires the performance of periodic reconciliations to verify that information uploaded from Clarity is recorded correctly in E1, and any adjustments to that information are complete and accurate.

Without such reconciliations, there is an increased risk of employees being paid incorrectly or their leave not being recorded properly.

> We recommend the Department carry out periodic reconciliations to ensure that hours in Clarity are uploaded properly to E1, and all adjustments thereto are accurate.

Department Response: DAS will review procedures to ensure hours in Clarity are uploaded completely and accurately to EnterpriseOne.

9. Shared Services Payroll Support

The Department of Health and Human Services (DHHS) and the Department of Veterans' Affairs (DVA) used the Kronos payroll application to track employee hours worked and leave used. DHHS and the DVA were responsible for the employee hours worked and leave used entered in the system and for supervisory approval of hours recorded in Kronos. DHHS and the DVA had a memorandum of agreement with the Department's Shared Services to process the payroll after supervisor approval.

The Department's Shared Services was responsible for: 1) performing the interface of Kronos hours to E1 in order to process employee pay; 2) reviewing reports to ensure all the hours recorded in Kronos were recorded in E1; 3) making adjustments to the E1 hours, as directed by DHHS and the DVA in the event corrections were necessary; and 4) processing the final payroll in E1 and setting up user access in the Kronos application.

During testing of two DVA biweekly pay periods, it was noted that one employee was underpaid $174 for work performed. The employee was underpaid for 7.25 overtime hours, 7 shift differential hours, and 0.25 regular hours that were recorded in Kronos but were not paid on E1. The Department responded that these hours were recorded to a non-payroll business unit that caused the error during the interface.

In addition, two DVA payment errors were made by the Department:

- One employee was overpaid $193 for 16 holiday hours earned on Thanksgiving and Black Friday, which were paid on both the January 3, 2020, and February 14, 2020, paychecks. The 16 hours should have been paid only once.

- One employee was underpaid $334. The Department recorded an incorrect adjustment that reduced the employee's hours from 40 to 9.6, which caused an underpayment of 30.4 hours.

Each of the two DHHS biweekly pay periods tested included 15 separate DHHS locations. For 2 of the 30 locations tested, the Department had not saved the documentation to support that the DHHS Kronos data was uploaded completely to E1.

Additionally, one DVA employee, who terminated on September 13, 2019, was included on the list of active Super Users provided on April 22, 2020. We noted also that one DHHS employee had access to make changes to pay rules for DHHS service areas, which was not part of her job function.

Good internal control requires procedures to ensure that data from Kronos is uploaded completely and accurately to E1, and documentation is maintained to support that a reconciliation of the interface data was performed. Those same procedures should ensure also that adjustments made to uploaded hours are accurate, and access to application systems is restricted to those who require it as part of their job function.

Without such procedures, there is an increased risk of an error in employee pay not being detected in a timely manner and improper activity taking place within the information system.

> We recommend the Department strengthen its procedures for ensuring that Kronos hours are uploaded completely and accurately to E1, and documentation is maintained to support that a reconciliation of the interface data was performed. Those same procedures should ensure also that adjustments made to E1 hours are accurate, and Kronos access is restricted to users based on their respective job functions.

Department Response: A data verification is performed based on the number of records loaded from Kronos into EnterpriseOne. DAS will review procedures for ensuring those hours are complete and accurate. A review of user access will be performed.

10. E1 Deposit Batches

During testing of controls within E1, we noted that users with approval access in the receipting queue were able to change a deposit after the deposit batch had been prepared by a user and then approve the transaction without a secondary review and approval.

Good internal control requires procedures to ensure that a proper segregation of duties exists, so no single individual is able to adjust and to approve a deposit without a secondary review by someone else.

The lack of such procedures increases the risk of an individual perpetrating and concealing errors, irregularities, or fraud.

> We recommend the Department implement procedures to ensure no one individual is able to adjust and to approve a deposit amount without a secondary review by someone else.

Department Response: The EnterpriseOne IT team will review available options for restricting the approver access that allows deposit batches to be changed without a secondary review.

11. State Employee and Vendor Address Book Issues

The APA conducted a detailed analysis of State employees and vendors within E1 to identify potentially fictitious employees, fraudulent payments, and internal control deficiencies.

E1 maintains detailed information about each State employee and vendor, which is categorized by an assigned address book number. This unique identification number can also be used to query certain information or run reports for a specific employee or vendor in the system.

In order to perform a detailed analysis, the APA ran reports and queries from E1 to obtain detailed listings of active and terminated employees, as well as vendors doing business with the State of Nebraska. This data was exported to a separate database, where the APA performed queries to identify potential risk areas for further review. For example, the APA ran queries to identify any duplicate address book numbers, tax identification numbers, or bank accounts, which could potentially identify fictitious employees.

The APA's detailed analysis of State employees and vendors within E1 revealed multiple issues, including invalid address book numbers and address book numbers missing key data elements, such as a bank account, tax identification number, mailing address, or date of birth. The APA has summarized these issues below.

Invalid or Missing Tax IDs

The APA's testing of employee and vendor tax identification numbers (tax ID) revealed that 210 vendors did not have a valid tax ID entered into E1. During the fiscal year ended June 30, 2020, these vendors were paid $778,612 and may be required to have an IRS Form 1099 issued, which would require a tax ID.

It was also noted that 32 of these vendors had text (e.g., "FOREIGN") entered in the tax ID field in E1. These vendors received $401,519 during the fiscal year.

The "Information Returns" Section of Internal Revenue Service (IRS) Publication 15 (2020), "Employer's Tax Guide," (Circular E), contains the following:

> *You [employers] may also be required to file information returns to report certain types of payments made during the year. For example, you must file Form 1099-MISC, Miscellaneous Income, to report payments of $600 or more in 2019 to persons not treated as employees (for example, independent contractors) for services performed for your trade or business.*

Furthermore, good internal control requires procedures to ensure that accurate tax identification information is entered into E1 for all vendors subject to the United States tax code.

Without such procedures, there is an increased risk of violating Federal tax law due to the resulting inability to file an IRS Form 1099.

> We recommend the Department implement procedures to ensure that all vendors covered under the United States tax code have an accurate tax identification number associated with their address book number in E1.

Department Response: DAS will review procedures for retaining accurate vendor and/or employee tax identification information in EnterpriseOne.

No Bank Account Information

As part of our detailed analysis, the APA identified the following issues with bank account information in E1:

- Two active employees did not have a bank account associated with their address book numbers.

- Three active Military Department contingent employees did not have a bank account associated with their address book numbers; however, these address book numbers had not received a paycheck in the last five years and had an inactive pay status in the system. Therefore, the address book numbers should be terminated in E1.

Good internal control requires procedures to ensure that complete and accurate information is maintained in E1 for all active employees in order to prevent the creation of fictitious employees.

Without such procedures, there is an increased risk of fraud or misuse of State funds.

> We recommend the Department implement procedures to ensure all active employee address book numbers are associated with an accurate bank account.

Department Response: DAS will review procedures for maintaining accurate bank account information for active employees and ensuring inactive records are set to the proper search type.

Invalid Active Employee Address Book Numbers

The APA noted three employee address book numbers that were active within E1 but should have been terminated or removed from the system. Two of the three address book numbers were not associated with an actual, active employee. The third address book number was for an employee already identified with a separate address book number in E1; therefore, the duplicate should be removed.

Good internal control requires procedures to ensure that active employee address book numbers are assigned to actual, active employees. Those same procedures should ensure also that, upon a separation of employment, the address book number is terminated to prevent misuse of the ID.

Without such procedures, there is an increased risk of fraud or misuse of State funds.

> We recommend the Department implement procedures to ensure active employee address book numbers are assigned to actual, active employees and terminated in E1 when a separation of employment occurs.

Department Response: DAS will review procedures for changing employee address book numbers to a terminated search type upon separation of employment.

No Mailing Addresses

Seven active employees did not have mailing addresses associated with their address book numbers at the time of testing.

Good internal control requires procedures to ensure that E1 contains complete and accurate mailing address information for all active employees.

Without such procedures, there is an increased risk of fraud or misuse of State funds due to the possibility of payments being made to fictitious employees.

> We recommend the Department implement procedures to ensure all active employees have complete and accurate mailing addresses in E1.

Department Response: DAS will review procedures for receiving and retaining accurate mailing addresses in EnterpriseOne.

Incorrect or Blank Dates of Births

The APA noted that 33 active employees did not have dates of birth associated with their address book numbers in E1 at the time of testing. Furthermore, two active employees had incorrect dates of birth associated with their address book numbers in the system; these individuals were assigned a default date of January 1, 1910, which would make both of them over 110 years old at the time of testing.

Good internal control requires procedures to ensure that complete and accurate birthday information is included for all employees in E1.

Without such procedures, there is an increased risk of fraud or misuse of State funds due to the possibility of payments being made to fictitious employees.

> We recommend the Department implement procedures to ensure accurate and complete dates of birth are entered into E1 for all active employees.

Department Response: DAS will review procedures for receiving and retaining accurate dates of birth for employees in EnterpriseOne.

* * * * * *

Our audit procedures are designed primarily on a test basis and, therefore, may not bring to light all weaknesses in policies or procedures that may exist. Our objective is, however, to use our knowledge of the Department and its interaction with other State agencies and administrative departments gained during our work to make comments and suggestions that we hope will be useful to the Department.

This communication is intended solely for the information and use of the Department, the Governor and State Legislature, others within the Department, Federal awarding agencies, pass-through entities, and management of the State of Nebraska and is not intended to be, and should not be, used by anyone other than the specified parties. However, this communication is a matter of public record, and its distribution is not limited.

Zachary Wells, CPA, CISA
Audit Manager